WHAT IS CLAIMED IS:

1. A method for issuing a portable electronic device containing an application program, comprising the steps of:

providing a security function against unauthorized use into the device, wherein the security function is validated by a command received from outside the device;

storing in the device data necessary to use the application program; and

validating the security function by issuing the command after storing said data.

2. The method of claim 1, wherein storing said data includes the step of:

storing a PIN code used to identify the owner of the device.

3. The method of claim 1, wherein:

said providing a security function comprises providing a plurality of security functions different from each other depending on corresponding application programs; and

said storing data comprises storing a cryptographic key used to identify a corresponding application program.

4. A portable electronic device containing an application program, comprising:

means for executing a security function against unauthorized use, the security function is validated by a command received from outside the device;

means for storing data necessary to use the application program; and

means for storing data indicating whether the security function is valid based on the command.

5. The device of claim 4, wherein:

said data necessary to use the application program is a PIN code used to identify the owner of the device.

6. The device of claim 4, wherein:

said security function executing means executes a plurality of security functions different from each other depending on corresponding application programs; and

said data necessary to use the application program is a cryptographic key to identify a corresponding application program.

7. The device of claim 4, wherein:

said portable electronic device is an IC card.

8. A portable electronic device with a security function, containing an application program, comprising:

a nonvolatile memory;

means for storing validity data indicating whether the security function is valid into the nonvolatile memory, wherein the validity data is received as a command message from the outside of the device;

first means for determining whether a command message provided from outside the device includes data for the security function;

second means for determining whether the nonvolatile memory is stored with the validity data; and

first means for writing or rewriting data into the nonvolatile memory following the command message, when the first determining means determines the command message does not include the data for security function, and, wherein the second determining means determines the nonvolatile memory not to be stored with the validity data.

9. The device of claim 8, further comprising:

first means for outputting a status indicating that the command message is not acceptable, when the first determining means determines the command message not to be including the data for security function, besides, when the second determining means determines the nonvolatile memory to be stored with the validity data.

10. The device of claim 8, further comprising:

third means for determining whether verification of the data for the security function succeeds, when the first determining means determines the command message to be including data for the security function; and

second means for writing or rewriting data into the nonvolatile memory following the command message, when the third determining means determines the verification is successful.

11. The device of claim 9, further comprising:

second means for outputting a status indicating that the command message is not acceptable when the third determining means determines the verification of the data for the security function is not successful.

12. The device of claim 9 wherein the command message comprises:

a writing or rewriting command;

data to be written or rewritten into the nonvolatile memory; and

additional data guaranteeing the justifiability of the data based on verification of the data.

13. The device of claim 9 wherein the command message comprises:

a writing or rewriting command; and

encoded data to be written or rewritten into the nonvolatile memory after being decoded, based on verification of the data.

14. The device of claim 9 wherein the command message comprises:

a writing or rewriting command;

encoded data to be written or rewritten into the nonvolatile memory after being decoded;

additional data guaranteeing the justifiability of the data; and wherein:

the verification of the data is performed based on the encoded data and the additional data.

15. The device of claim 9, wherein the nonvolatile memory stores a plurality of security programs different from each other depending on a corresponding application program.

16. The device of claim 13, wherein each security program is separately validated in response to a prescribed command message for validation, and wherein each security program corresponds to an application program.

17. The device of claim 13, wherein at least one available format of the command message is separately defined, and wherein each format corresponds to an application program.